

(19) 世界知的所有権機関  
国際事務局



(43) 国際公開日  
2004 年11 月18 日 (18.11.2004)

PCT

(10) 国際公開番号  
WO 2004/100456 A1

(51) 国際特許分類<sup>7</sup>: H04L 12/46, 12/66, G06F 15/00

(21) 国際出願番号: PCT/JP2004/003327

(22) 国際出願日: 2004 年3 月12 日 (12.03.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:  
特願2003-132904 2003 年5 月12 日 (12.05.2003) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒1410001 東京都品川区北品川 6 丁目 7 番 3 5 号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 中野 雄彦 (NAKANO, Takehiko) [JP/JP]; 〒1410001 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社内 Tokyo

(JP). 高林 和彦 (TAKABAYASHI, Kazuhiko) [JP/JP]; 〒1410001 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社内 Tokyo (JP). 本田 康晃 (HONDA, Yasuaki) [JP/JP]; 〒1410001 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社内 Tokyo (JP). 五十嵐 卓也 (IGARASHI, Tatsuya) [JP/JP]; 〒1410001 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社内 Tokyo (JP).

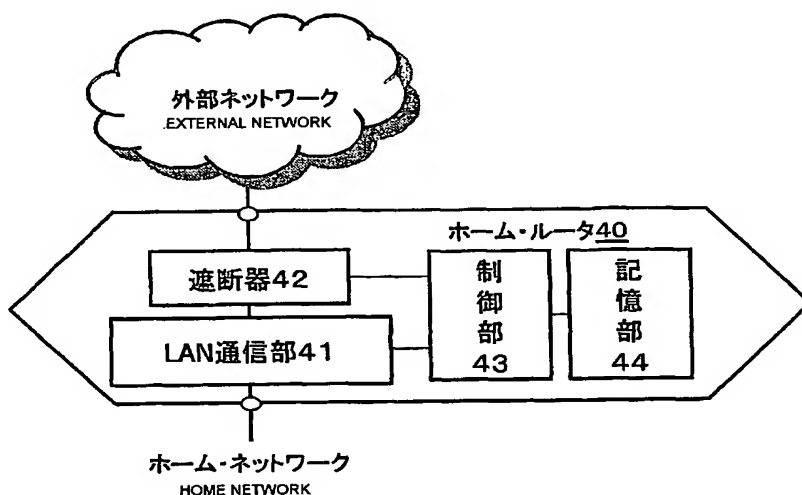
(74) 代理人: 山田 英治, 外 (YAMADA, Eiji et al.); 〒1040041 東京都中央区新富一丁目 1 番 7 号 銀座ティーケイビル 澤田・宮田・山田特許事務所 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG,

[続葉有]

(54) Title: INTER-DEVICE AUTHENTICATION SYSTEM, INTER-DEVICE AUTHENTICATION METHOD, COMMUNICATION DEVICE, AND COMPUTER PROGRAM

(54) 発明の名称: 機器間認証システム及び機器間認証方法、通信機器、並びにコンピュータ・プログラム



42...CUT-OFF DEVICE

41...LAN COMMUNICATION SECTION

40...HOME ROUTER

43...CONTROL SECTION

44...STORAGE SECTION

(57) Abstract: A function for isolating a home network from an external network is mounted on a router or a gateway arranged between the home network and the external network. For example, when a home server registers a client as a member or providing a content or issuing the license, the home network is isolated from the external network so that it is guaranteed that the request source client can exist in a local environment. It is possible to manage use of the content validly acquired on the home server, within a private use range admitted by the copyright law, by the client terminal.

[続葉有]



SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ,  
VC, VN, YU, ZA, ZM, ZW.

- (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

- 国際調査報告書
- 補正書・説明書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約: ホーム・ネットワークと外部ネットワークの間に介在するルータ又はゲートウェイにホーム・ネットワークを外部ネットワークから隔離する機能を装備し、例えばホーム・サーバがクライアントをメンバー登録したり、コンテンツの提供又はそのライセンスを発行したりするときに、ホーム・ネットワークを外部ネットワークから隔離することによって、要求元クライアントがローカル環境に存在することを保証する。ホーム・サーバ上で正当に取得されているコンテンツを著作権法で認められる私的使用の範囲内でクライアント端末が利用するように管理することができる。

## 1

## 明 細 書

機器間認証システム及び機器間認証方法、通信機器、並びにコンピュータ・プログラム

5

## 技術分野

本発明は、ネットワークなどによって配信される音楽データや画像データ、電子出版物などのデジタル・データや動画像などコンテンツの利用を管理する機器  
10 間認証システム及び機器間認証方法、通信機器、並びにコンピュータ・プログラムに係り、特に、著作権法で認められる私的使用の範囲内でコンテンツの利用を管理する機器間認証システム及び機器間認証方法、通信機器、並びにコンピュータ・プログラムに関する。

さらに詳しくは、本発明は、ルータ経由で外部ネットワークに接続されている  
15 ホーム・ネットワーク上で、著作権法で認められる私的使用の範囲内でコンテンツの利用を管理する機器間認証システム及び機器間認証方法、通信機器、並びにコンピュータ・プログラムに係り、特に、ホーム・ネットワーク上の各クライアント端末がホーム・サーバ上で正当に取得されているコンテンツを著作権法で認められる私的使用の範囲内で利用するように管理する機器間認証システム及び機  
20 器間認証方法、通信機器、並びにコンピュータ・プログラムに関する。

## 背景技術

近年のインターネットの普及により、コンピュータ・ファイルを始めとした各  
25 種のデジタル・コンテンツをネットワーク配信することが盛んに行なわれている。また、広帯域通信網(xDSL(x Digital Subscriber Line)、CATV(Cable TV)、無線ネットワークなど)の普及により、音楽データや画像データ、電子出版物などのデジタル・データや、さらには動画像などリッチ・コンテンツの配信もユーザにストレスなく伝送できるような仕組

みが整いつつある。

一方、配信されるコンテンツはデジタル・データであり、コピーや改竄などの不正な操作を比較的容易に行なうことができる。また、現在これらのコンテンツのコピーや改竄などの不正行為は頻繁に行なわれており、これがデジタル・コンテンツ・ベンダの利益を阻害する主要な要因となっている。この結果、コンテンツの値段も高くしなければならなくなり、普及の障壁となるという悪循環が起きている。

例えば、最近では一般家庭内にもコンピュータやネットワークなどの技術が深く浸透してきている。家庭内のパーソナル・コンピュータやPDA (Personal Digital Assistants) などの情報機器、さらにはテレビ受像機やビデオ再生装置などの各種の情報家電がホーム・ネットワーク経由で相互接続されている。また、このようなホーム・ネットワークは、多くの場合、ルータ経由でインターネットを始めとする外部の広域ネットワークに相互接続されている。そして、インターネット上のサーバから正当に取得されたコンテンツは、ホーム・ネットワーク上のサーバ（以下、「ホーム・サーバ」とも呼ぶ）に蓄積された後、家庭内の他の端末（クライアント）へホーム・ネットワーク経由で配信される。

著作権法の下、著作物としてのコンテンツは無断の複製や改竄などの不正使用から保護を受ける。一方、著作物の正当な利用者においては、私的な使用、すなわち個人的に又は家庭内その他これに準ずる限られた範囲内において使用することを目的としてコンテンツを複製することが許されている（著作権法第30条を参照のこと）。

この私的使用の範囲を上述したホーム・ネットワークにおいて適用した場合、ホーム・ネットワークに接続されているクライアント端末は、個人的又は家庭の範囲内での使用であると推定される。したがって、ホーム・サーバにおいて正当に取得されているコンテンツは、ホーム・ネットワーク上のクライアント端末は自由に使用することが相当であると思料される（勿論、コンテンツを享受できる端末の台数に一定の制限を設ける必要がある）。

しかしながら、ホーム・ネットワーク上にログインしたクライアント端末が私

的使用の範囲にあるかどうかを識別することは、現状の技術では困難である。

例えば、ホーム・ネットワークはルータを介して外部のネットワークと I P プ  
ロトコル・ベースで相互接続されていることから、ホーム・サーバにとってはア  
クセスしてきたクライアントが実際にどこにいるのかは不明である。外部（遠隔）  
5 からのアクセスに対しホーム・サーバがコンテンツを提供してしまうと、コンテ  
ンツの利用はほぼ無制限となってしまう、コンテンツに関する著作権は保護され  
ないに等しい。この結果、コンテンツ製作者は創作意欲を失いかねない。

また、ホーム・サーバがホーム・ネットワーク内のクライアント端末に対して  
一様にコンテンツの利用を許可した場合、同じクライアント端末が時間差をおい  
10 て複数のホーム・ネットワークに跨ってログインすることにより、ほぼ無尽蔵に  
コンテンツを利用することが可能となってしまう。

他方、クライアント端末に対して厳しい制限を課してしまうと、ユーザは、本  
来著作権法上で認められている私的使用を確保することができなくなってしまう。  
この結果、ユーザがコンテンツを十分に享受することができず、ホーム・サーバ  
15 やコンテンツ配信サービスの利用が進まないために、コンテンツ事業の発展自体  
を阻害しかねない。

例えば、著作物を正規に購入した利用者に自由利用が認められているというこ  
とに鑑み、利用者がネットワーク上での情報を複製して利用するにあたって、コ  
ンテンツの権利保持者の理解が得られ易い方法に関する提案がなされている（例  
20 えば、特開 2 0 0 2 - 7 3 8 6 1 号公報を参照のこと）。しかしながら、これは利  
用者を情報の利用権保持者との関係レベルによって分類し、関係レベル毎に異な  
る配信方法で情報を配信するというもので、ネットワーク上のどこまでが私的使  
用の範囲にあるかを識別するものではない。

また、最近では、ホーム・ネットワークを構成するプロトコルとして、例えば  
25 U P n P（登録商標）が知られている。U P n P によれば、複雑な操作を伴うこ  
となく容易にネットワークを構築することが可能であり、ネットワーク接続され  
た機器間では困難な操作や設定を伴うことなくコンテンツ提供サービスを行なう  
ことが可能となる。また、U P n P は、オペレーティング・システム（O S）に  
非依存であり、容易に機器の追加ができるという利点を持つ。

UPnPでは、ネットワーク接続された機器間で、XML (eXtended Markup Language) 形式で記述された定義ファイルを交換して相互認証を行なう。UPnPの処理の概要は以下の通りである。

- (1) アドレッシング処理：IPアドレスなどの自己のデバイスIDを取得する
- 5 (2) ディスカバリ処理：ネットワーク上の各デバイスの検索を行ない、各デバイスから受信した応答に含まれるデバイス種別や機能などの情報を取得する
- (3) サービス要求処理：ディスカバリ処理で取得された情報に基づいて各デバイスにサービスを要求する

このような処理手順を行なうことで、ネットワーク接続された機器を適用した  
10 サービスの提供並びに受領が可能となる。新たにネットワークに接続される機器は、アドレッシング処理によりデバイスIDを取得し、ディスカバリ処理によりネットワーク上の他のデバイスについての情報を取得し、サービス要求が可能となる。

ホーム・サーバに格納されたコンテンツは、ホーム・ネットワーク上の他の機器からアクセス可能となる。例えば、UPnP接続を実行した機器によってコンテンツを取得することが可能である。コンテンツが映像データや音声データの場合、ネットワーク接続機器として、TVやプレーヤなどを接続すれば、映画や音楽を視聴することができる。

しかし、ホーム・ネットワーク内の機器、例えばホーム・サーバには私的なコンテンツや有料コンテンツなど著作権管理を要求されるコンテンツが格納されていることから、不正アクセスの対策を考慮する必要がある。

コンテンツの利用権（ライセンス）を有するユーザの機器によるアクセスは許容されて当然である。しかしながら、ホーム・ルータ経由で外部ネットワークに相互接続されているホーム・ネットワーク環境では、ライセンスを持たないユーザがホーム・ネットワークに入り込むことも可能である。

不正アクセスを排除するため、例えば、ホーム・サーバにアクセスを許容するクライアントのリストを保持させ、クライアントからホーム・サーバへのアクセス要求が行なわれる度に、リストとの照合処理を実行して、不正アクセスを排除することができる。

例えば、各通信機器に固有の物理アドレスであるMAC (Media Access Control) アドレスを用いてアクセス許容機器リストとして設定するMACアドレス・フィルタリングが知られている。すなわち、ホーム・ネットワークのような内部ネットワークと外部ネットワークとを隔離するルータ又はゲートウェイにアクセスを許容する各機器のMACアドレスを登録しておき、受信したパケットに付されているMACアドレスと登録されたMACアドレスとを照合し、未登録のMACアドレスを持つ機器からのアクセスを拒否する(例えば、特開平10-271154号公報を参照のこと)。

しかしながら、アクセス許容機器リストを構築するためには、内部ネットワークに接続されるすべての機器のMACアドレスを調べる必要があり、また、取得したすべてのMACアドレスを入力してリストを作成する手間が必要である。また、ホーム・ネットワークにおいては、接続される機器が比較的頻繁に変更され、かかる変更の度にアクセス許容機器リストを修正しなければならない。

## 15 発明の開示

本発明の目的は、ルータ経由で外部ネットワークに接続されているホーム・ネットワーク上でのコンテンツの利用を好適に管理することができる、優れた機器間認証システム及び機器間認証方法、通信機器、並びにコンピュータ・プログラムを提供することにある。

本発明のさらなる目的は、ホーム・ネットワーク上の各クライアント端末がホーム・サーバ上で正当に取得されているコンテンツを著作権法で認められる私的使用の範囲内で利用するように好適に管理することができる、優れた機器間認証システム及び機器間認証方法、通信機器、並びにコンピュータ・プログラムを提供することにある。

本発明は、上記課題を参酌してなされたものであり、その第1の側面は、ルータ経由で外部ネットワークに接続されているホーム・ネットワーク上の機器を認証する機器間認証システムであって、

## 6

前記外部ネットワークと前記ホーム・ネットワーク間の経路を接続・遮断する経路遮断手段と、

- 前記ホーム・ネットワーク上の機器間で通信を行なうことを保証するタイミングにおいて、前記経路遮断手段を作動させて前記ホーム・ネットワークを前記外部ネットワークから隔離して、前記ホーム・ネットワーク内でのローカル通信を実現するローカル環境管理手段と、
- 5 前記ホーム・ネットワーク内でのローカル通信を実現するローカル環境管理手段と、
- を具備することを特徴とする機器間認証システムである。

- 但し、ここで言う「システム」とは、複数の装置（又は特定の機能を実現する機能モジュール）が論理的に集合した物のことを言い、各装置や機能モジュール
- 10 が単一の筐体内にあるか否かは特に問わない。

- ここで、一方の機器は前記ルータ経由で外部ネットワークからコンテンツを正当に取得するホーム・サーバであり、他方の機器はホーム・サーバに対してコンテンツを要求し利用するクライアントである。そして、双方の機器が同じホーム・ネットワーク上に存在することが確認されたことに応じて、前記ホーム・サーバ
- 15 は前記クライアントに対しコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なう。

- 著作権法の下、著作物としてのコンテンツは無断の複製や改竄などの不正使用から保護を受ける。一方、著作物の正当な利用者においては、私的な使用、すなわち個人的に又は家庭内その他これに準ずる限られた範囲内において使用すること
- 20 を目的としてコンテンツを複製することが許されている。

- 前記ホーム・ネットワーク上には2台以上のホーム・サーバを設置可能である。このような場合、各ホーム・サーバは、同じホーム・ネットワーク上のクライアント端末はローカル環境下にあることから、それぞれ独自にこれらをメンバー登録してグループを形成し、コンテンツ配信並びにコンテンツ使用のライセンスを発
- 25 行する。さらに、クライアント端末は、同じホーム・ネットワーク上の2台以上のホーム・サーバに対し同時にメンバー登録し複数のグループに所属し、各々のホーム・サーバからコンテンツのライセンスを取得することができる。

この場合も、クライアント端末は、それぞれのホーム・サーバにとってローカル環境下に存在し、個人的又は家庭の範囲内での使用であると推定されるから、



ローカル環境内の各ホーム・サーバのコンテンツを自由に使用することが相当である。

一方、クライアント端末が複数のホーム・サーバに同時にメンバー登録できるからといって、時間差を置いて、複数のホーム・ネットワークに跨って複数のホーム・サーバのグループに所属することまでは認めるべきでない。別のホーム・ネットワークに接続した時点で、元の接続先のホーム・ネットワークから見ればクライアント端末がリモート環境に移動したことに相当し、あるいは、あるホーム・ネットワークに接続した時点で他のホーム・ネットワークにとってクライアント端末はリモート環境に存在することに等しいからである。

したがって、本発明に係る機器間認証システムでは、クライアントは、同じホーム・ネットワーク上の複数のホーム・サーバから取得したコンテンツを利用可能であるが、別のホーム・ネットワーク上のホーム・サーバに接続した時点で、それ以外のホーム・ネットワーク上のホーム・サーバから取得したコンテンツを利用不能となるようにする。

現状のネットワーク・プロトコルでは、ネットワーク経由で相互接続されている機器同士が真正すなわち個人的又は家庭の範囲内でコンテンツを私的使用できるかどうかを識別する仕組みは提供されていない。そこで、本発明では、ホーム・ネットワークと外部ネットワークの経路を一時的に遮断することにより、その期間において通信し合える機器が同じホーム・ネットワーク上に存在することを保証するようにした。

本発明によれば、ホーム・ネットワークと外部ネットワークの経路を遮断したり接続したりする制御機構を例えばホーム・ルータに装備する。そして、ホーム・サーバがクライアント端末をメンバー登録したり、コンテンツの提供やそのライセンスの発行を行ったりするなど、ローカル環境下での通信であることを保証しなければならないタイミングにおいて、ホーム・ネットワークと外部ネットワークとの経路を遮断する。この結果、ホーム・サーバがローカル通信を行ない、ローカル環境下に存在するクライアント端末のみがホーム・サーバ上に蓄積されているコンテンツを利用することができるようになる。

前記ホーム・ネットワーク上でのローカル通信が完了後、又はローカル通信を

開始してから所定時間経過後に、前記ホーム・ネットワークと前記外部ネットワーク間の経路を再開させればよい。

5 また、本発明の第2の側面は、ルータ経由で外部ネットワークに接続されているホーム・ネットワーク上の機器を認証するための処理をコンピュータ・システム上で実行するようにコンピュータ可読形式で記述されたコンピュータ・プログラムであって、

前記ホーム・ネットワーク上の機器間で通信を行なうことを保証するタイミングを取得するステップと、

10 該タイミングにおいて、前記外部ネットワークと前記ホーム・ネットワーク間の経路を一時的に遮断して前記ホーム・ネットワークを前記外部ネットワークから隔離せしめるステップと、

を具備することを特徴とするコンピュータ・プログラムである。

15 本発明の第2の側面に係るコンピュータ・プログラムは、コンピュータ・システム上で所定の処理を実現するようにコンピュータ可読形式で記述されたコンピュータ・プログラムを定義したものである。換言すれば、本発明の第2の側面に係るコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の第1の側面に係る機器間認証システムと同様の作用効果を得ることができる。

20

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施形態や添付する図面に基づくより詳細な説明によって明らかになるであろう。

#### 図面の簡単な説明

25

図1は、ホーム・ネットワークの基本構成を模式的に示した図である。

図2は、2台のホーム・サーバが存在するホーム・ネットワークの構成例を示した図である。

図3は、クライアント端末が複数のホーム・ネットワークに跨って接続する様

子を示した図である。

図4は、本発明の一実施形態に係るホーム・ネットワークの構成を模式的に示した図である。

5 図5は、本発明の他の実施形態に係るホーム・ネットワークの構成を模式的に示した図である。

図6は、サーバやクライアントなどとしてホーム・ネットワークに接続されるホスト装置のハードウェア構成を模式的に示した図である。

図7は、ホーム・ネットワークと外部ネットワークを接続するホーム・ルータ40の内部構造を示した図である。

10 図8は、ホーム・ネットワークと外部ネットワークを接続するホーム・ルータ40の内部構造についての他の実現例を示した図である。

図9は、ホーム・ルータ40によるホーム・ネットワークと外部ネットワークとの経路遮断を行なうための処理手順を示した動作シーケンス図である。

15 発明を実施するための最良の形態

以下、図面を参照しながら本発明の実施形態について詳解する。

20 著作権法の下、著作物としてのコンテンツは無断の複製や改竄などの不正使用から保護を受ける。一方、著作物の正当な利用者においては、私的な使用、すなわち個人的に又は家庭内その他これに準ずる限られた範囲内において使用することを目的としてコンテンツを複製することが許されている（著作権法第30条を参照のこと）。

25 本発明者らは、ホーム・ネットワーク内（以下、「ローカル環境」とも呼ぶ）のクライアント端末は、私的な使用の範囲内にあるという前提に立ち、ローカル環境下のクライアントに限り、ホーム・サーバ上に蓄積されているコンテンツを利用することができるというシステムを提案する。

ここで、ローカル環境の定義について説明しておく。

図1には、ホーム・ネットワークの基本構成を模式的に示している。同図に示

すように、家庭内に敷設されるホーム・ネットワークは、ホーム・ルータ経由でインターネットなどの外部ネットワークに接続されている。

ホーム・ネットワーク上には、ホーム・サーバと、1以上のクライアント端末が存在する。ホーム・サーバは、ホーム・ルータ経由で外部ネットワーク上のコンテンツ・サーバから正当にコンテンツを取得し、蓄積し、家庭内でコンテンツを配信する。勿論、ホーム・サーバは、パッケージ・メディアや放送受信など、ネットワーク以外の手段により、コンテンツを取得することができる。また、各クライアント端末は、ホーム・サーバに所望のコンテンツを要求し、これを取得して利用する。

10 ホーム・ネットワークに接続されているクライアント端末は、ローカル環境下に存在し、個人的又は家庭の範囲内での使用であると推定される。したがって、ホーム・サーバにおいて正当に取得されているコンテンツは、ホーム・ネットワーク上のクライアント端末は自由に使用することが相当であると思料される。

そこで、ホーム・サーバは、ローカル環境下のこれらクライアント端末をメンバー登録し、コンテンツ配信並びにコンテンツ使用のライセンスを発行する。勿論、コンテンツを享受できる端末の台数に一定の制限を設ける必要がある。

ローカル環境下では、クライアント端末は、ホーム・サーバからコンテンツを取得し、コピーやストリーミングなどコンテンツを利用し、さらにローカル環境外（リモート環境）にコンテンツを持ち出して利用することができる。

20 一方、ホーム・ネットワーク上に存在しない、すなわちリモート環境のクライアント端末は、個人的又は家庭の範囲内での使用であるとは考えられない。リモート環境のクライアント端末にコンテンツの利用を認めると、コンテンツの利用はほぼ無制限となってしまう、コンテンツに関する著作権は保護されないに等しくなるからである。そこで、ホーム・サーバは、リモート環境のクライアントをメンバーとして登録せず、また、コンテンツのライセンスを発行しない。

25 図1に示した例では、ホーム・ネットワーク上には1つのホーム・サーバしか存在しないが、勿論、2以上のホーム・サーバを同じホーム・サーバ上に設置して、各ホーム・サーバがホーム・ネットワーク内でそれぞれ独自にコンテンツの配信サービスを行なうようにしてもよい。

図2には、2台のホーム・サーバが存在するホーム・ネットワークの構成例を示している。

この場合、各ホーム・サーバは、同じホーム・ネットワーク上のクライアント端末はローカル環境下にあることから、これらをメンバー登録してグループを形成し、コンテンツ配信並びにコンテンツ使用のライセンスを発行する。クライアント端末は、ホーム・サーバからコンテンツを取得し、コピーやストリーミングなどコンテンツを利用し、さらにローカル環境外（リモート環境）にコンテンツを持ち出して利用することができる。

さらに、クライアント端末は、同じホーム・ネットワーク上の2台以上のホーム・サーバに対し同時にメンバー登録し複数のグループに所属し、各々のホーム・サーバからコンテンツのライセンスを取得することができる。この場合も、クライアント端末は、それぞれのホーム・サーバにとってローカル環境下に存在し、個人的又は家庭の範囲内での使用であると推定されるから、ローカル環境内の各ホーム・サーバのコンテンツを自由に使用することが相当であると思料される。

一方、クライアント端末が複数のホーム・サーバに同時にメンバー登録できるからといって、複数のホーム・ネットワークに跨って複数のホーム・サーバのグループに所属することまでは認めるべきでない（図3を参照のこと）。何故ならば、別のホーム・ネットワークに接続した時点で、元の接続先のホーム・ネットワークから見ればクライアント端末がリモート環境に移動したことに相当し、あるいは、あるホーム・ネットワークに接続した時点で他のホーム・ネットワークにとってクライアント端末はリモート環境に存在することに等しいからである。ローカル環境が個人的又は家庭の範囲内であるのに対し、リモート環境は個人的又は家庭の範囲を逸脱する。

クライアント端末が時間差をかけて複数のホーム・ネットワークに跨って接続することは技術的には可能であるが、これに併せてコンテンツの利用を逐次許可していくと、コンテンツの利用はほぼ無制限となってしまう、コンテンツに関する著作権は保護されないに等しくなる。

以上を総括すると、ホーム・ネットワーク上において、個人的又は家庭の範囲内での使用であると推定されるローカル環境を実現するためには、以下の事柄が

必要条件であることが導出される。

(1) ホーム・サーバは、ホーム・ネットワーク外からのメンバー登録を認めない。

- 5 (2) 同じホーム・ネットワーク内に2台以上のホーム・サーバがあるときには、ホーム・サーバ毎にメンバー登録、グループ管理を行なう。ホーム・ネットワーク上の各クライアントは2以上のホーム・サーバに登録することができる。但し、同時登録されるホーム・サーバは同じホーム・ネットワークに存在しなければならない。

- 10 このようなローカル環境を実現するためには、ホーム・サーバとクライアント端末間で、お互い同じホーム・ネットワーク上に存在するかどうかを識別する仕組みが必要となる。

- 15 現状のネットワーク・プロトコルでは、ホーム・ネットワークなどネットワークをセグメント単位で識別する仕組みは提供されていない。そこで、本発明者らは、ホーム・ネットワークと外部ネットワークの間に介在するルータ又はゲートウェイにホーム・ネットワークを外部ネットワークから隔離する機能を装備し、例えばホーム・サーバがクライアントをメンバー登録したり、コンテンツの提供又はそのライセンスを発行したりするときに、ホーム・ネットワークを外部ネットワークから隔離又は遮断することによって、要求元クライアントがホーム・サーバと同じローカル環境に存在することを保証する、という方法を提案する。

- 20 図4には、本発明の一実施形態に係るホーム・ネットワークの構成を模式的に示している。

- 25 家庭内に敷設されるホーム・ネットワークは、ホーム・ルータ経由でインターネットなどWAN、あるいは他のLANに接続されている。ホーム・ネットワークのデフォルト・ゲートウェイ (default Gateway) はホーム・ルータに設定されている。

ホーム・ネットワークは、例えばハブ (集結装置) にホーム・サーバやクライアント端末などのホスト装置のLANケーブルを接続することにより構成される。

ホーム・サーバやクライアント端末、ホーム・ルータなどのホーム・ネットワーク上のホスト装置、並びに外部ネットワーク上のホスト装置は、機器固有のM

ACアドレスを有している。ホスト装置は、受信先MACアドレス及び送信元MACアドレスを含んだヘッダ情報を持つパケット、例えばイーサネット（登録商標）フレームを、ネットワーク経由で送受信する。

5      ホーム・サーバやクライアント端末などのホーム・ネットワーク上のホスト装置は、例えばUPnP対応機器として構成される。この場合、ネットワークに対する接続機器の追加や削除が容易である。ホーム・ネットワークに新たに接続する機器は、以下の手順に従って、コンテンツ利用などホーム・ネットワーク上のサービスを享受することができるようになる。

- 10      (1) アドレッシング処理：IPアドレスなどの自己のデバイスIDを取得する  
    (2) ディスカバリ処理：ネットワーク上の各デバイスの検索を行ない、各デバイスから受信した応答に含まれるデバイス種別や機能などの情報を取得する  
    (3) サービス要求処理：ディスカバリ処理で取得された情報に基づいて各デバイスにサービスを要求する

15      ホーム・ネットワーク上では、個人的又は家庭の範囲内での使用であると推定されるローカル環境が形成されている。したがって、ホーム・サーバは、ホーム・ルータ経由で外部ネットワーク上のコンテンツ・サーバから正当にコンテンツを取得し、蓄積し、家庭内でコンテンツを配信する。また、各クライアント端末は、ホーム・サーバに所望のコンテンツを要求し、これを取得して利用することが許容される。

20      ローカル環境下では、クライアント端末は、ホーム・サーバからコンテンツを取得し、コピーやストリーミングなどコンテンツを利用し、さらにローカル環境外（リモート環境）にコンテンツを持ち出して利用することができる。

また、図5には、本発明の他の実施形態に係るホーム・ネットワークの構成を模式的に示している。

25      ホーム・ネットワークは、ホーム・ルータ経由でインターネットなどWAN、あるいは他のLANに接続されている。この場合も、ホーム・ネットワークのdefault Gatewayはホーム・ルータに設定されている。

図4との相違は、ホーム・ネットワーク上に2台のホーム・サーバが存在する点である。各ホーム・サーバは、ホーム・ネットワーク上に同時に存在してもよ

いし、あるいは時間差を以って接続されてもよい。

この場合、各ホーム・サーバは、同じホーム・ネットワーク上のクライアント端末はローカル環境下にあることから、これらをメンバー登録してグループを形成し、コンテンツ配信並びにコンテンツ使用のライセンスを発行する。クライアント端末は、ホーム・サーバからコンテンツを取得し、コピーやストリーミングなどコンテンツを利用し、さらにローカル環境外（リモート環境）にコンテンツを持ち出して利用することができる。また、クライアント端末は、同じホーム・ネットワーク上の2台以上のホーム・サーバに対し同時にメンバー登録し複数のグループに所属し、各々のホーム・サーバからコンテンツのライセンスを取得することができる。

図6には、サーバやクライアントなどとしてホーム・ネットワークに接続されるホスト装置のハードウェア構成を模式的に示している。

このシステムは、プロセッサ10を中心に構成されている。プロセッサ10は、メモリに記憶されたプログラムに基づいて各種の処理を実行する。また、プロセッサは、バス30を介して接続されている各種の周辺機器を制御している。バス30に接続された周辺機器は次のようなものである。

メモリ20は、例えばDRAM (Dynamic RAM) などの半導体メモリで構成され、プロセッサ10において実行されるプログラム・コードをロードしたり、実行プログラムの作業データを一時格納したりするために使用される。

ディスプレイ・コントローラ21は、プロセッサ10から送られてくる描画命令に従って表示画像を生成し、表示装置22に送る。ディスプレイ・コントローラに接続された表示装置22は、ディスプレイ・コントローラ21から送られた表示画像情報に従い、その画像を画面に表示出力する。

入出力インターフェース23は、キーボード24やマウス25が接続されており、キーボード24やマウス25からの入力信号をバス30経由でプロセッサ10へ転送する。

ネットワーク・インターフェース26は、ホーム・ネットワーク（ハブ）に接続され、さらにホーム・ルータ40経由でインターネットなどの外部ネットワークに接続されており、インターネットを介したデータ通信を制御する。すなわち、



プロセッサ10から送られたデータをインターネット上の他の装置へ転送するとともに、インターネットを介して送られてきたデータを受け取りプロセッサ10に渡す。

- ハード・ディスク装置 (HDD: Hard Disk Drive) コントローラ27には、HDDなどの大容量外部記憶装置28が接続されており、HDD コントローラ27が接続されたHDD28へのデータの入出力を制御する。HDD 28には、プロセッサが実行すべきオペレーティング・システム (OS) のプログラム、アプリケーション・プログラム、ドライバ・プログラムなどが格納されている。アプリケーション・プログラムは、例えば、ホーム・サーバとしてホーム・ネットワーク上の各クライアント端末の認証処理を行ったり、コンテンツの提供やライセンスの発行を行ったりするサーバ・アプリケーションや、サーバから提供されたコンテンツの再生などコンテンツの利用を行なうクライアント・アプリケーションなどである。

- なお、ホスト装置を構成するためには、図6に示した以外にも多くの電気回路などが必要である。但し、これらは当業者には周知であり、また、本発明の要旨を構成するものではないので、本明細書中では省略している。また、図面の錯綜を回避するため、図中の各ハードウェア・ブロック間の接続も一部しか図示していない点を了承されたい。

- 図7には、ホーム・ネットワークと外部ネットワークを接続するホーム・ルータ40の内部構造を示している。LAN通信部41は、ホーム・サーバとの通信を行なうための送受信機能である。遮断器42は、ホーム・ネットワークをWANなどの外部ネットワークと隔離又は遮断する機能モジュールである。制御部43は、LAN通信部41を通じた通信をコントロールし、ホーム・サーバとの認証の実施や、制御メッセージの交換、遮断器42の制御などを行なう。記憶部44は、制御部43の動作プログラムやそのために必要なデータ、認証のための鍵情報などを蓄積する。

また、図8には、ホーム・ルータ40の別の実装形態を示している。同図に示す構成では、遮断器42で外部ネットワークとホーム・ネットワークを切り離した状態でも、ホーム・ルータ40はWAN通信部45によって外部ネットワーク

との通信が可能である。この場合、例えば、他に外部ネットワークと通信している装置が存在しないかを監視したり、さらに別の装置、例えば別のモデムに対して外部ネットワークとの経路遮断を指示したり、その指示通りに通信が遮断されているかを、実際に外部ネットワーク上の所定のサーバへのアクセスを試すことで確認するといったことをWAN通信部45を利用して行なうことで、より確実に遮断を実現することができる。

図9には、ホーム・ルータ40によるホーム・ネットワークと外部ネットワークとの経路遮断を行なうための処理手順を示している。

10 ホーム・サーバは、クライアント端末をホーム・ネットワーク内のグループのメンバーとして登録したり、私的にのみ利用可能なコンテンツ又はそのライセンスをクライアント端末に提供したりする段階で、クライアント端末がローカル環境すなわち同じホーム・ネットワーク上に存在することを確保しなければならない。

15 このようにローカルな通信が必要になった段階で、ホーム・サーバはホーム・ルータ40に対し、外部ネットワークへの経路の遮断を依頼する。

経路遮断に先立って、ホーム・ルータ40が依頼通りに働く正当な機器であることを確認するため、認証処理を行なうようにしてもよい。但し、一般のUPnP対応ルータのように、遮断の制御はできても認証機能は持たないケースもあり得るので、認証処理は必須ではない。

20 この認証には、例えば、一般的なチャレンジ・レスポンス認証などが適用される。この場合、ホーム・サーバから乱数をホーム・ルータ40に送り、これに対し、ホーム・ルータ40はホーム・サーバと共有する秘密鍵を乱数に連結してハッシュ化したものを求め、ホーム・サーバに返送する。ホーム・サーバは、同様の方法でホーム・ルータ40が返送してくる筈の期待値を求め、一致が確認されれば認証を成功とする。このような共有秘密鍵ベースの方法の他に、公開鍵ベースの、ホーム・ルータ40の秘密鍵で暗号化して返送するという方法もある。

25 認証成功後は、ホーム・サーバからホーム・ルータ40に経路の遮断を指示する。このようにして、ホーム・ネットワークが外部ネットワークから隔離又は遮断された状態で、ホーム・サーバはクライアント端末をホーム・ネットワーク内

のグループのメンバーとして登録したり、私的にのみ利用可能なコンテンツ又はそのライセンスをクライアント端末に提供したりするなどのローカル通信を行なう。

- クライアント端末は、ホーム・サーバと同じローカル環境に存在する場合にのみ、メンバー登録やコンテンツ又はそのライセンスの提供をうけることができ、外部ネットワークからのなりすましを防止することができる。ローカル環境内においてのみ機器間でコンテンツの利用を認めることにより、コンテンツの不正流通を効果的に抑制することができる。

- その後、ホーム・サーバからホーム・ルータに経路の再開を指示することによって、ホーム・ネットワークと外部ネットワーク間を遮断していた経路を復活させる。

- 但し、ローカル通信を行なう期間中ホーム・ネットワークを外部ネットワークから遮断する必要はない。例えば、ローカル通信を開始してから所定時間だけホーム・ネットワークを外部ネットワークから隔離することによっても、クライアント端末がローカル環境に存在することを保証することができる。したがって、ホーム・ネットワークと外部ネットワーク間の経路の再開は、ホーム・ルータ 40 がホーム・サーバからの指示（コマンド）に応答して行なうのではなく、経路を遮断してから所定時間経過後に自律的に経路の再開を行なうように構成してもよい。

- なお、認証成功後の上記制御についても、第 3 者によるなりすましを防ぐため、認証を通じて鍵を共有し、その鍵で制御通信を保護するという方法もある。例えば、前記ハッシュ化した結果を、認証に使う部分と鍵として使う部分に分けて、鍵は制御通信のメッセージのハッシュ化に使う。そして、このハッシュ化の結果を制御メッセージとともに送ることで、受信した装置における同様のハッシュ処理によるメッセージの正当性チェックが可能である。

また、図 9 に示した動作シーケンス例では、ホーム・ルータ 40 は、ホーム・サーバからの明示的な指示（自身宛のコマンド）に応答して、ホーム・ネットワークと外部ネットワーク間の経路の遮断を実行するようになっているが、ホーム・ルータ 40 が自律的に経路の遮断を行なうように構成することもできる。例

例えば、ホーム・ルータ 40 は、LAN 通信部 41 を通じてホーム・ネットワーク上の動作（すなわち、ネットワーク上の転送コマンド）を常時監視し、ホーム・サーバがクライアント端末をホーム・ネットワーク内のグループのメンバーとして登録したり、私的にのみ利用可能なコンテンツ又はそのライセンスをクライアント端末に提供したりするなどのローカル通信を行なうタイミングを検出し、このようなタイミングにおいて自律的に経路の遮断動作を起動する。この場合、勿論、ホーム・ルータ 40 が自律的に経路の再開を行なうように構成してもよい。

### 追捕

- 10 以上、特定の実施形態を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施形態の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、本明細書の記載内容を限定的に解釈すべきではない。本発明の要旨を判断するためには、特許請求の範囲の欄を参酌すべきである。

15

### 産業上の利用可能性

- 20 本発明によれば、ルータ経由で外部ネットワークに接続されているホーム・ネットワーク上でコンテンツの利用を好適に管理することができる、優れた機器間認証システム及び機器間認証方法、通信機器、並びにコンピュータ・プログラムを提供することができる。

- 25 また、本発明によれば、ホーム・ネットワーク上の各クライアント端末がホーム・サーバ上で正当に取得されているコンテンツを著作権法で認められる私的使用の範囲内で利用するように好適に管理することができる、優れた機器間認証システム及び機器間認証方法、通信機器、並びにコンピュータ・プログラムを提供することができる。

本発明によれば、ローカル環境内においてのみ機器間でコンテンツの利用を認めることにより、コンテンツの不正流通を効果的に抑制することができる。

## 請求の範囲

1. ルータ経由で外部ネットワークに接続されているホーム・ネットワーク上の機器を認証する機器間認証システムであって、

- 5 前記外部ネットワークと前記ホーム・ネットワーク間の経路を接続・遮断する経路遮断手段と、

前記ホーム・ネットワーク上の機器間で通信を行なうことを保証するタイミングにおいて、前記経路遮断手段を作動させて前記ホーム・ネットワークを前記外部ネットワークから隔離するローカル環境管理手段と、

- 10 を具備することを特徴とする機器間認証システム。

2. 一方の機器は前記ルータ経由で前記外部ネットワークからコンテンツを正当に取得するホーム・サーバであり、他方の機器は前記ホーム・サーバに対してコンテンツを要求し利用するクライアントであり、

- 15 前記ローカル環境管理手段により前記ホーム・ネットワークを前記外部ネットワークから隔離した状態で、前記ホーム・サーバは前記クライアントに対しコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なう、ことを特徴とする請求項1に記載の機器間認証システム。

- 20 3. 前記ホーム・ネットワーク上には2台以上のホーム・サーバを設置可能であり、

前記ローカル環境管理手段は、ホーム・サーバ毎にクライアントに対しコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なう際に、前記外部ネットワークと前記ホーム・ネットワーク間の経路を一時的に遮断する、

- 25 ことを特徴とする請求項1に記載の機器間認証システム。

4. クライアントは、同じホーム・ネットワーク上の2台以上のホーム・サーバからコンテンツの提供及び／又はコンテンツに関するライセンスの発行を受けることができる、

ことを特徴とする請求項 3 に記載の機器間認証システム。

5. クライアントは、同じホーム・ネットワーク上の複数のホーム・サーバから取得したコンテンツを利用可能であるが、別のホーム・ネットワーク上のホーム・

- 5 サーバに接続した時点で、それ以外のホーム・ネットワーク上のホーム・サーバから取得したコンテンツを利用不能となる、

ことを特徴とする請求項 3 に記載の機器間認証システム。

6. 前記ローカル環境管理手段は、前記ホーム・ネットワーク上でのローカル通信が完了後、又はローカル通信を開始してから所定時間経過後に、前記ホーム・ネットワークと前記外部ネットワーク間の経路を再開させる、

- 10 ことを特徴とする請求項 1 に記載の機器間認証システム。

7. ルータ経由で外部ネットワークに接続されているホーム・ネットワーク上の機器を認証する機器間認証方法であって、

- 15 前記ホーム・ネットワーク上の機器間で通信を行なうことを保証するタイミングにおいて、前記外部ネットワークと前記ホーム・ネットワーク間の経路を一時的に遮断して前記ホーム・ネットワークを前記外部ネットワークから隔離する、ことを特徴とする機器間認証方法。

20

8. 一方の機器は前記ルータ経由で外部ネットワークからコンテンツを正当に取得するホーム・サーバであり、他方の機器はホーム・サーバに対してコンテンツを要求し利用するクライアントであり、

前記ホーム・ネットワークを前記外部ネットワークから隔離した状態で、前記

- 25 ホーム・サーバは前記クライアントに対しコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なう、ことを特徴とする請求項 7 に記載の機器間認証方法。

9. 前記ホーム・ネットワーク上には 2 台以上のホーム・サーバを設置可能であ

り、

ホーム・サーバ毎に、クライアントに対しコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なう際に、前記外部ネットワークと前記ホーム・ネットワーク間の経路を一時的に遮断する、

5      ことを特徴とする請求項 7 に記載の機器間認証方法。

10      10. クライアントは、同じホーム・ネットワーク上の 2 台以上のホーム・サーバからコンテンツの提供及び／又はコンテンツに関するライセンスの発行を受けることができる、

10      ことを特徴とする請求項 9 に記載の機器間認証方法。

15      11. クライアントは、同じホーム・ネットワーク上の複数のホーム・サーバから取得したコンテンツを利用可能であるが、別のホーム・ネットワーク上のホーム・サーバに接続した時点で、それ以外のホーム・ネットワーク上のホーム・サーバから取得したコンテンツを利用不能となる、

15      ことを特徴とする請求項 9 に記載の機器間認証方法。

20      12. 前記ホーム・ネットワーク上でのローカル通信が完了後、又はローカル通信を開始してから所定時間経過後に、前記ホーム・ネットワークと前記外部ネッ

20      トワーク間の経路を再開させる、

20      ことを特徴とする請求項 7 に記載の機器間認証方法。

25      13. ルータ経由で外部ネットワークに接続されているホーム・ネットワーク上で動作する通信機器であって、

25      前記ホーム・ネットワーク上の機器間で通信を行なうことを保証するタイミングにおいて、前記ホーム・ネットワークを前記外部ネットワークから遮断することを要求するローカル環境管理手段を備える、

25      ことを特徴とする通信機器。

1 4. ホーム・ネットワーク上でコンテンツを提供するホーム・サーバとして動作し、

前記ローカル環境管理手段は、クライアントに対しコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なう際に、前記ホーム・ネットワーク

- 5    クを前記外部ネットワークから遮断することを要求する、  
ことを特徴とする請求項 1 3 に記載の通信機器。

1 5. 前記ローカル環境管理手段は、クライアントとのローカル通信の終了後、前記ホーム・ネットワークと前記外部ネットワークとの接続を再開することを要

- 10    求する、  
ことを特徴とする請求項 1 4 に記載の通信機器。

1 6. ホーム・ネットワークと外部ネットワークを相互接続する通信機器であって、

- 15    前記外部ネットワークと前記ホーム・ネットワーク間の経路を接続・遮断する経路遮断手段と、

前記ホーム・ネットワーク上の機器間で通信を行なうことを保証するタイミングにおいて、前記経路遮断手段を作動させて前記ホーム・ネットワークを前記外部ネットワークから隔離する制御手段と、

- 20    を具備することを特徴とする通信機器。

1 7. 前記制御手段は、前記ホーム・ネットワーク上でコンテンツを提供するホーム・サーバからの遮断要求に応じて前記ホーム・ネットワークを前記外部ネットワークから隔離する、

- 25    ことを特徴とする請求項 1 6 に記載の通信機器。

1 8. 前記制御手段は、前記ホーム・ネットワーク上でコンテンツを提供するホーム・サーバからの再開要求に応じて、遮断中の前記ホーム・ネットワークと前記外部ネットワークの接続を再開する、



ことを特徴とする請求項 16 に記載の通信機器。

19. 前記制御手段は、前記ホーム・ネットワーク上でコンテンツを提供するホーム・サーバからの遮断要求に応じて前記ホーム・ネットワークを前記外部ネットワークから隔離した後、所定のタイミングで前記ホーム・ネットワークと前記外部ネットワークの接続を再開する、
- 5 ことを特徴とする請求項 16 に記載の通信機器。

20. 前記ホーム・ネットワークと前記外部ネットワークを遮断中に、前記外部ネットワークと通信する手段と、
- 10 前記ホーム・ネットワークと前記外部ネットワークを遮断中に、前記外部ネットワーク上の所定のサーバにアクセスして、前記ホーム・ネットワークと前記外部ネットワークとの経路が遮断していることを確認する手段と、
- をさらに備えることを特徴とする請求項 16 に記載の通信機器。

15

21. ルータ経由で外部ネットワークに接続されているホーム・ネットワーク上の機器を認証するための処理をコンピュータ・システム上で実行するようにコンピュータ可読形式で記述されたコンピュータ・プログラムであって、

- 前記ホーム・ネットワーク上の機器間で通信を行なうことを保証するタイミングを取得するステップと、
- 20

該タイミングにおいて、前記外部ネットワークと前記ホーム・ネットワーク間の経路を一時的に遮断して前記ホーム・ネットワークを前記外部ネットワークから隔離せしめるステップと、

を具備することを特徴とするコンピュータ・プログラム。

## 補正書の請求の範囲

[2004年8月16日(16.08.04)国際事務局受理 : 出願当初の請求の範囲  
1、7、16及び21は補正された。他の請求の範囲は変更なし。(5頁)]

1. (補正後) ルータ経由で外部ネットワークに接続されているホーム・ネットワーク上の機器を認証する機器間認証システムであって、

5 前記外部ネットワークと前記ホーム・ネットワーク間の経路を接続・遮断する経路遮断手段と、

前記ホーム・ネットワーク上の機器間で通信を行なうことを保証するタイミングにおいて、前記ホーム・ネットワーク上の機器が発する要求に基づいて前記経路遮断手段を作動させて前記ホーム・ネットワークを前記外部ネットワークから

10 隔離するローカル環境管理手段と、  
を具備することを特徴とする機器間認証システム。

2. 一方の機器は前記ルータ経由で前記外部ネットワークからコンテンツを正当に取得するホーム・サーバであり、他方の機器は前記ホーム・サーバに対してコンテンツを要求し利用するクライアントであり、

15 前記ローカル環境管理手段により前記ホーム・ネットワークを前記外部ネットワークから隔離した状態で、前記ホーム・サーバは前記クライアントに対しコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なう、  
ことを特徴とする請求項1に記載の機器間認証システム。

20

3. 前記ホーム・ネットワーク上には2台以上のホーム・サーバを設置可能であり、

前記ローカル環境管理手段は、ホーム・サーバ毎にクライアントに対しコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なう際に、前記  
25 外部ネットワークと前記ホーム・ネットワーク間の経路を一時的に遮断する、  
ことを特徴とする請求項1に記載の機器間認証システム。

4. クライアントは、同じホーム・ネットワーク上の2台以上のホーム・サーバからコンテンツの提供及び／又はコンテンツに関するライセンスの発行を受ける

ことができる、

ことを特徴とする請求項 3 に記載の機器間認証システム。

- 5 5. クライアントは、同じホーム・ネットワーク上の複数のホーム・サーバから取得したコンテンツを利用可能であるが、別のホーム・ネットワーク上のホーム・サーバに接続した時点で、それ以外のホーム・ネットワーク上のホーム・サーバから取得したコンテンツを利用不能となる、  
ことを特徴とする請求項 3 に記載の機器間認証システム。

- 10 6. 前記ローカル環境管理手段は、前記ホーム・ネットワーク上でのローカル通信が完了後、又はローカル通信を開始してから所定時間経過後に、前記ホーム・ネットワークと前記外部ネットワーク間の経路を再開させる、  
ことを特徴とする請求項 1 に記載の機器間認証システム。

- 15 7. (補正後) ルータ経由で外部ネットワークに接続されているホーム・ネットワーク上の機器を認証する機器間認証方法であって、  
前記ホーム・ネットワーク上の機器間で通信を行なうことを保証するタイミングにおいて、前記ホーム・ネットワーク上の機器が発する要求に基づいて前記外部ネットワークと前記ホーム・ネットワーク間の経路を一時的に遮断して前記ホーム・ネットワークを前記外部ネットワークから隔離する、  
20 ことを特徴とする機器間認証方法。

8. 一方の機器は前記ルータ経由で外部ネットワークからコンテンツを正当に取得するホーム・サーバであり、他方の機器はホーム・サーバに対してコンテンツを要求し利用するクライアントであり、  
25

前記ホーム・ネットワークを前記外部ネットワークから隔離した状態で、前記ホーム・サーバは前記クライアントに対しコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なう、  
ことを特徴とする請求項 7 に記載の機器間認証方法。

9. 前記ホーム・ネットワーク上には2台以上のホーム・サーバを設置可能であり、

ホーム・サーバ毎に、クライアントに対しコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なう際に、前記外部ネットワークと前記ホーム・ネットワーク間の経路を一時的に遮断する、

5 ことを特徴とする請求項7に記載の機器間認証方法。

10. クライアントは、同じホーム・ネットワーク上の2台以上のホーム・サーバからコンテンツの提供及び／又はコンテンツに関するライセンスの発行を受けることができる、

10 ことを特徴とする請求項9に記載の機器間認証方法。

11. クライアントは、同じホーム・ネットワーク上の複数のホーム・サーバから取得したコンテンツを利用可能であるが、別のホーム・ネットワーク上のホーム・サーバに接続した時点で、それ以外のホーム・ネットワーク上のホーム・サーバから取得したコンテンツを利用不能となる、

15 ことを特徴とする請求項9に記載の機器間認証方法。

12. 前記ホーム・ネットワーク上でのローカル通信が完了後、又はローカル通信を開始してから所定時間経過後に、前記ホーム・ネットワークと前記外部ネットワーク間の経路を再開させる、

20 ことを特徴とする請求項7に記載の機器間認証方法。

13. ルータ経由で外部ネットワークに接続されているホーム・ネットワーク上で動作する通信機器であって、

25 前記ホーム・ネットワーク上の機器間で通信を行なうことを保証するタイミングにおいて、前記ホーム・ネットワークを前記外部ネットワークから遮断することを要求するローカル環境管理手段を備える、  
ことを特徴とする通信機器。

14. ホーム・ネットワーク上でコンテンツを提供するホーム・サーバとして動作し、

前記ローカル環境管理手段は、クライアントに対しコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なう際に、前記ホーム・ネットワーク

- 5     クを前記外部ネットワークから遮断することを要求する、  
ことを特徴とする請求項13に記載の通信機器。

15. 前記ローカル環境管理手段は、クライアントとのローカル通信の終了後、前記ホーム・ネットワークと前記外部ネットワークとの接続を再開することを要

- 10    求する、  
ことを特徴とする請求項14に記載の通信機器。

16. (補正後) ホーム・ネットワークと外部ネットワークを相互接続する通信機器であって、

- 15    前記外部ネットワークと前記ホーム・ネットワーク間の経路を接続・遮断する経路遮断手段と、

前記ホーム・ネットワーク上の機器間で通信を行なうことを保証するタイミングにおいて、前記ホーム・ネットワーク上の機器が発する要求に基づいて前記経路遮断手段を作動させて前記経路遮断手段を作動させて前記ホーム・ネットワー

- 20    クを前記外部ネットワークから隔離する制御手段と、  
を具備することを特徴とする通信機器。

17. 前記制御手段は、前記ホーム・ネットワーク上でコンテンツを提供するホーム・サーバからの遮断要求に応じて前記ホーム・ネットワークを前記外部ネッ

- 25    トワークから隔離する、  
ことを特徴とする請求項16に記載の通信機器。

18. 前記制御手段は、前記ホーム・ネットワーク上でコンテンツを提供するホーム・サーバからの再開要求に応じて、遮断中の前記ホーム・ネットワークと前

記外部ネットワークの接続を再開する、  
ことを特徴とする請求項 16 に記載の通信機器。

- 5 19. 前記制御手段は、前記ホーム・ネットワーク上でコンテンツを提供するホーム・サーバからの遮断要求に応じて前記ホーム・ネットワークを前記外部ネットワークから隔離した後、所定のタイミングで前記ホーム・ネットワークと前記外部ネットワークの接続を再開する、  
ことを特徴とする請求項 16 に記載の通信機器。

- 10 20. 前記ホーム・ネットワークと前記外部ネットワークを遮断中に、前記外部ネットワークと通信する手段と、  
前記ホーム・ネットワークと前記外部ネットワークを遮断中に、前記外部ネットワーク上の所定のサーバにアクセスして、前記ホーム・ネットワークと前記外部ネットワークとの経路が遮断していることを確認する手段と、  
15 をさらに備えることを特徴とする請求項 16 に記載の通信機器。

21. (補正後) ルータ経由で外部ネットワークに接続されているホーム・ネットワーク上の機器を認証するための処理をコンピュータ・システム上で実行するようにコンピュータ可読形式で記述されたコンピュータ・プログラムであって、  
20 前記ホーム・ネットワーク上の機器間で通信を行なうことを保証するタイミングを取得するステップと、  
該タイミングにおいて、前記ホーム・ネットワーク上の機器が発する要求に基づいて前記外部ネットワークと前記ホーム・ネットワーク間の経路を一時的に遮断して前記ホーム・ネットワークを前記外部ネットワークから隔離せしめるステップと、  
25 を具備することを特徴とするコンピュータ・プログラム。

## 条約第19条(1)に基づく説明書

請求の範囲第1項では、ローカル環境管理手段が「前記ホーム・ネットワーク上の機器が発する要求に基づいて」前記経路遮断手段を作動させて前記ホーム・ネットワークを前記外部ネットワークから隔離するという点を明確にした。

また、請求の範囲第7項では、「前記ホーム・ネットワーク上の機器が発する要求に基づいて」前記外部ネットワークと前記ホーム・ネットワーク間の経路を一時的に遮断して前記ホーム・ネットワークを前記外部ネットワークから隔離するという点を明確にした。

また、請求の範囲第16項では、制御手段が「前記ホーム・ネットワーク上の機器が発する要求に基づいて」前記ホーム・ネットワークを前記外部ネットワークから隔離する制御手段という点を明確にした。

また、請求の範囲第21項では、「前記ホーム・ネットワーク上の機器が発する要求に基づいて」前記外部ネットワークと前記ホーム・ネットワーク間の経路を一時的に遮断して前記ホーム・ネットワークを前記外部ネットワークから隔離せしめるステップという点を明確にした。

なお、本願明細書の第16頁第14行乃至同頁第15行には、「ローカルな通信が必要になった段階で、ホーム・サーバはホーム・ルータ40に対し、外部ネットワークへの経路の遮断を依頼する」という点が明記されている。

1/5

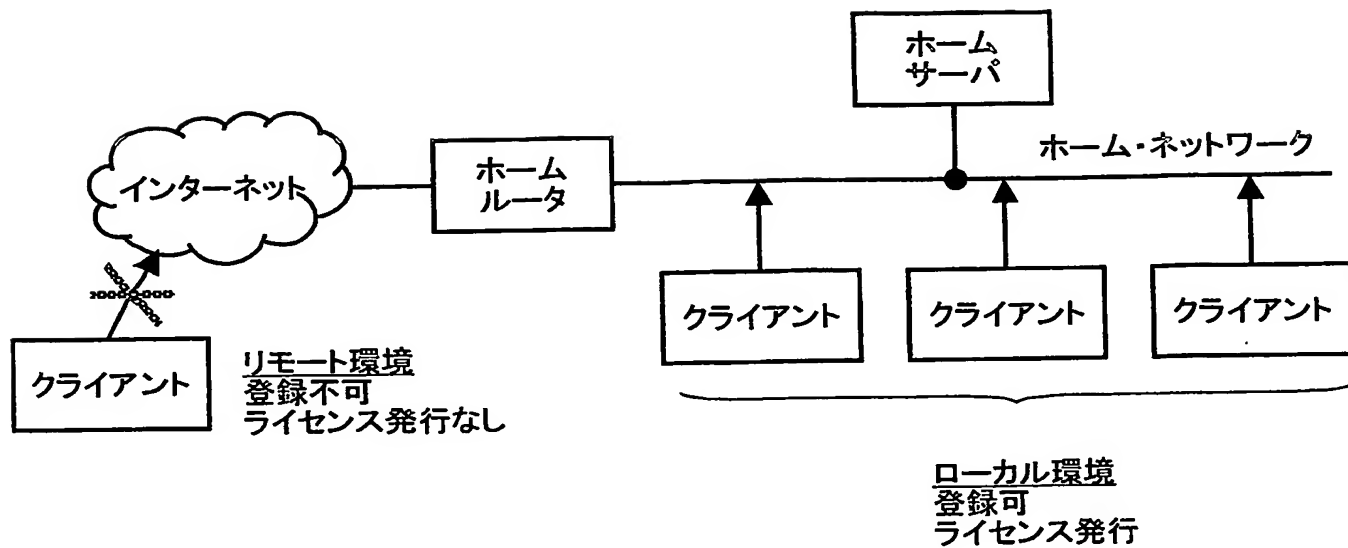


図1

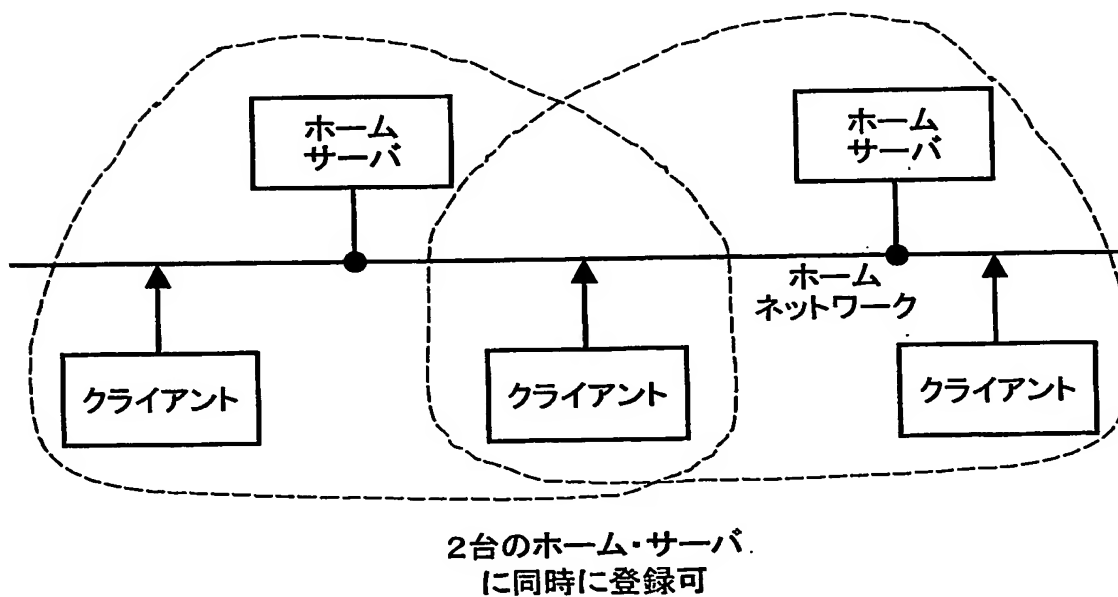


図2



2/5

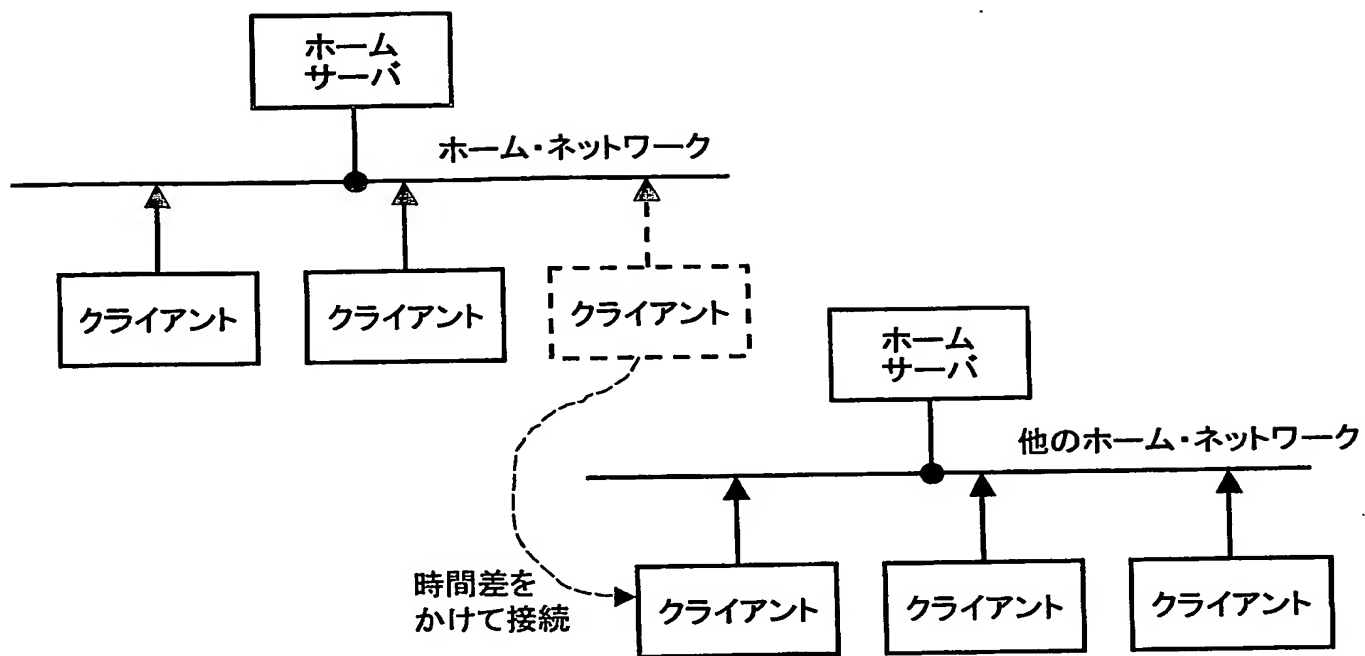


図3

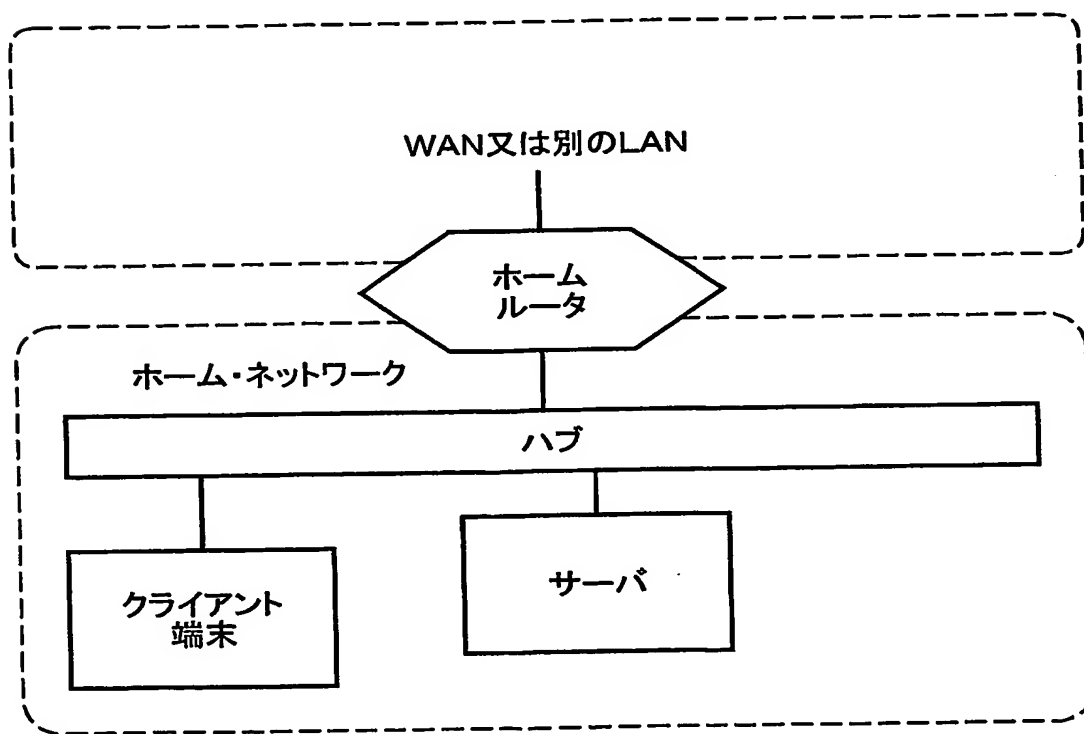


図4

3/5

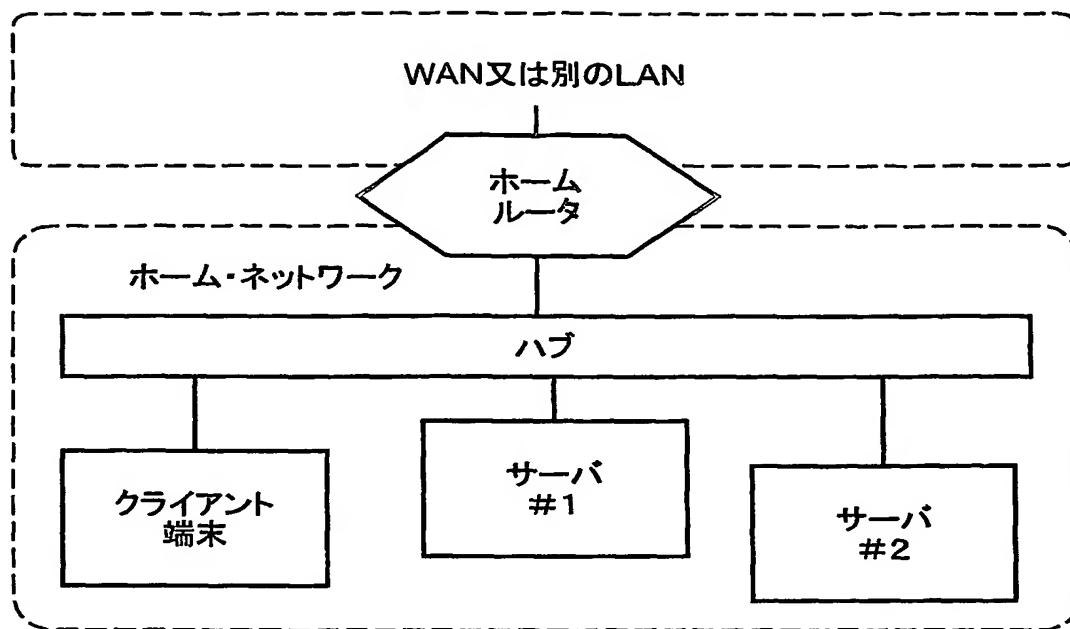


図5

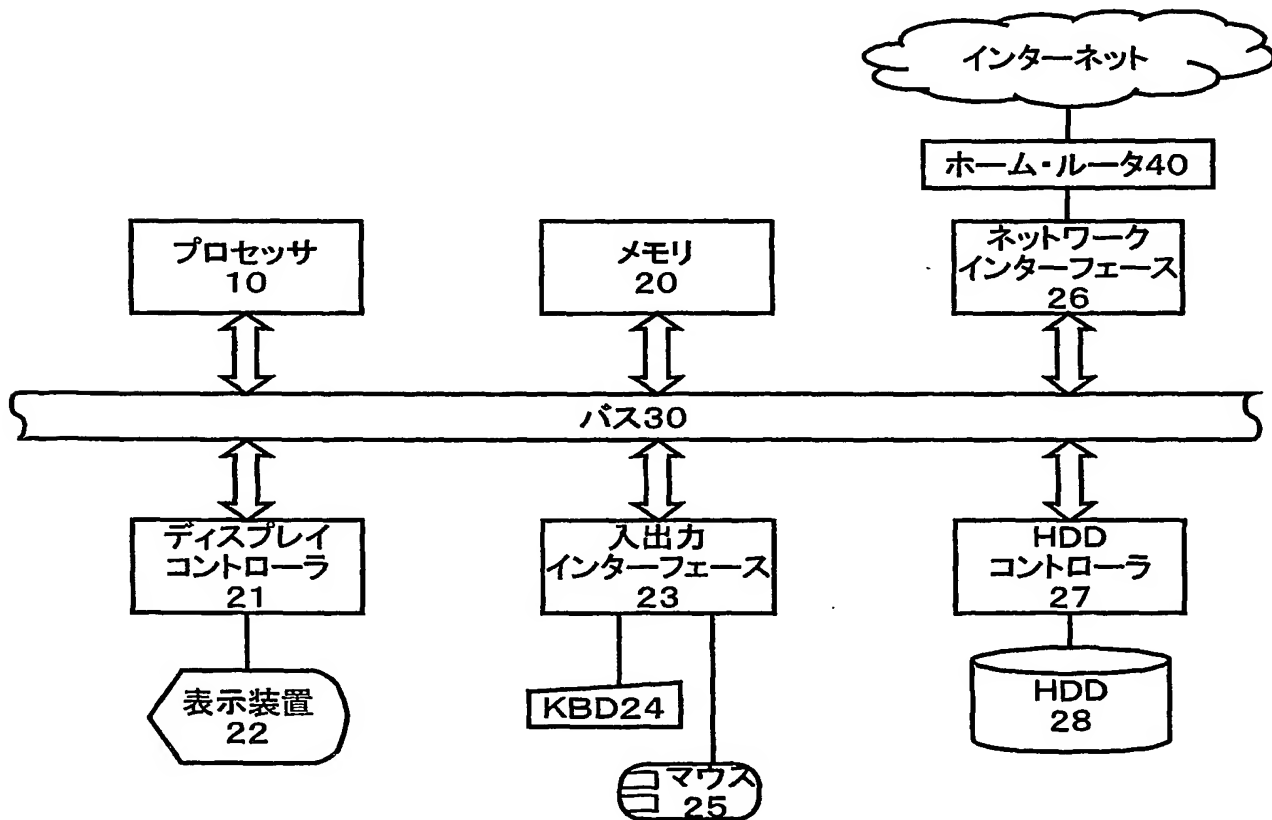


図6

4/5

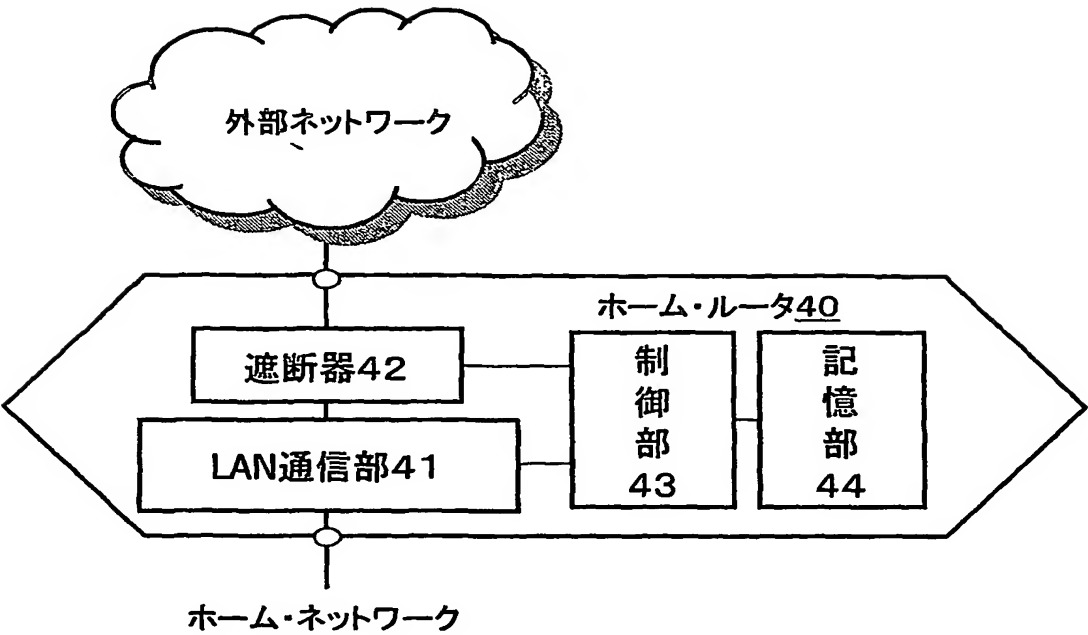


図7

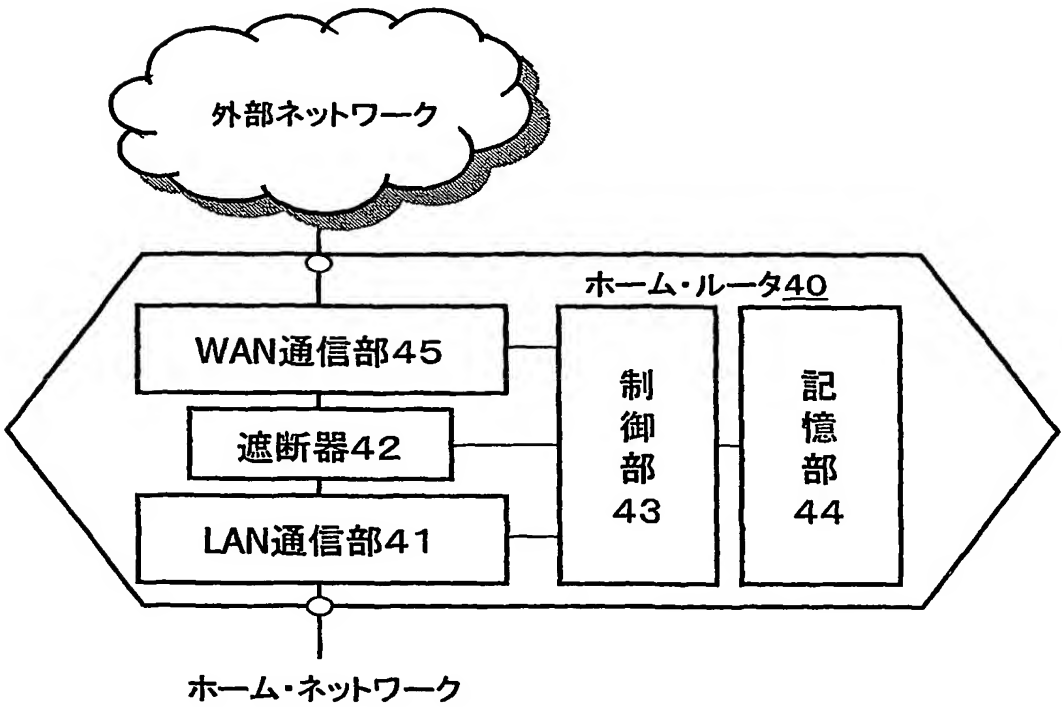


図8

5/5

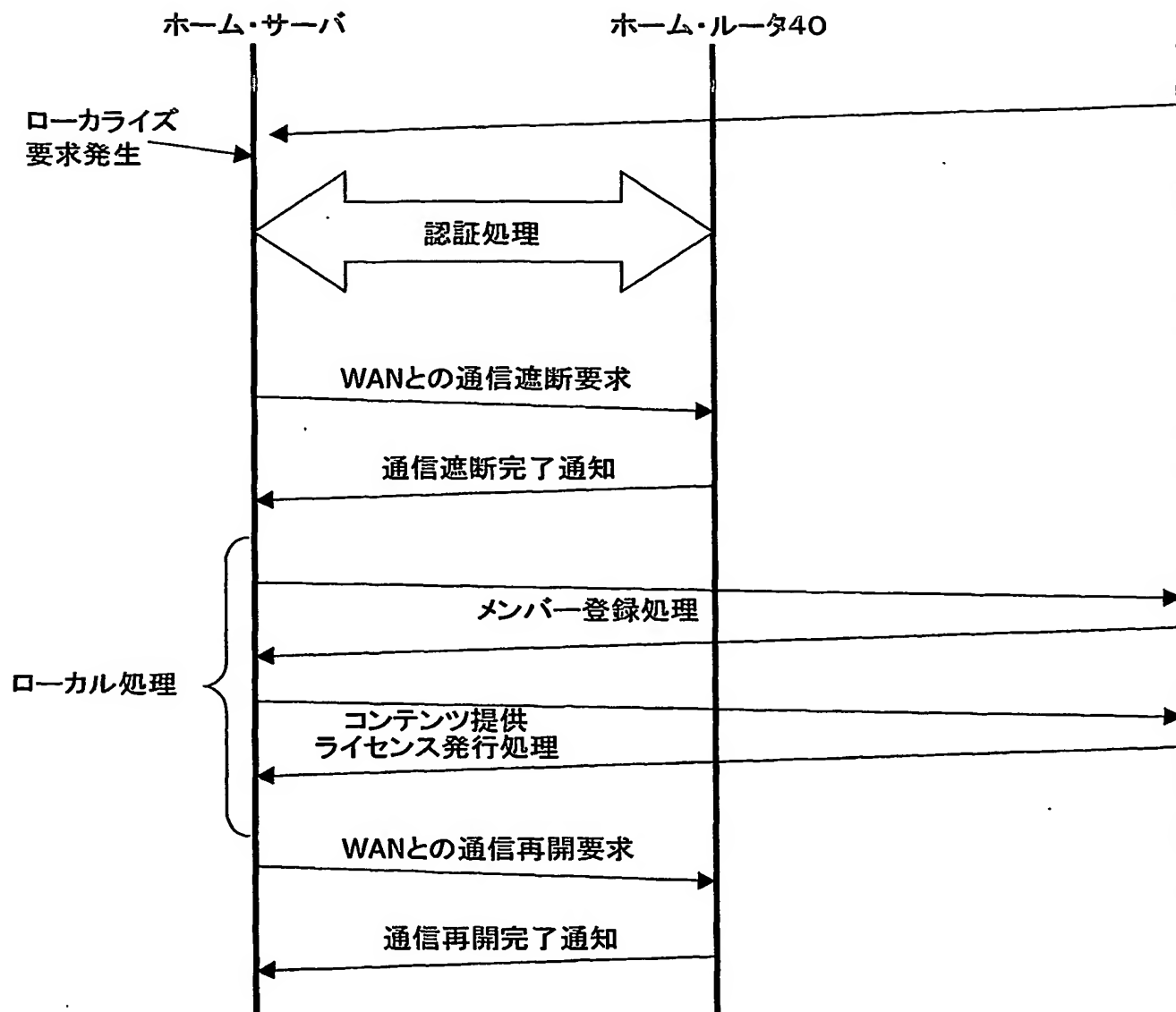


図9

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/003327

## A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl<sup>7</sup> H04L12/46, H04L12/66, G06F15/00

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl<sup>7</sup> H04L12/46, H04L12/66, G06F15/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2004

Kokai Jitsuyo Shinan Koho 1971-2004 Jitsuyo Shinan Toroku Koho 1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2002-175224 A (NEC Corp.), 21 June, 2002 (21.06.02), Par. Nos. [0023] to [0036]; Figs. 1 to 3 (Family: none)	1, 6, 7, 12, 16, 18, 21 2-5, 8-11 13-15, 17, 19-20
Y	JP 2002-007233 A (IONOS CO., LTD.), 11 January, 2002 (11.01.02), Par. Nos. [0044] to [0049] & EP 1164766 A2 & US 2001/0054159 A1	2-5, 8-11
Y	JP 2003-076805 A (International Business Machines Corp.), 14 March, 2003 (14.03.03), Par. No. [0027] (Family: none)	5-11

☐ Further documents are listed in the continuation of Box C.☐ See patent family annex.

\* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&amp;" document member of the same patent family

Date of the actual completion of the international search  
17 May, 2004 (17.05.04)Date of mailing of the international search report  
22 June, 2004 (22.06.04)Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

## A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl.<sup>7</sup> H04L12/46, H04L12/66, G06F15/00

## B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl.<sup>7</sup> H04L12/46, H04L12/66, G06F15/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年

日本国公開実用新案公報 1971-2004年

日本国登録実用新案公報 1994-2004年

日本国実用新案登録公報 1996-2004年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	JP 2002-175224 A (日本電気株式会社) 2002.06.21, 【0023】-【0036】, 図1-3 (ファミリーなし)	1, 6, 7, 12, 16, 18, 21
Y		2-5, 8-11
A		13-15, 17, 19-20

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの

「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」 口頭による開示、使用、展示等に言及する文献

「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&amp;」 同一パテントファミリー文献

国際調査を完了した日

17.05.2004

国際調査報告の発送日

22.6.2004

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

中木 努

5X

9299

電話番号 03-3581-1101 内線 3596

C (続き). 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 2002-007233 A (株式会社イオノス) 2002. 01. 11, 【0044】, 【0049】 & EP 1164766 A2 & US 2001/0054159 A1	2-5, 8-11
Y	JP 2003-076805 A (インターナショナル・ビジネ ス・マシーンズ・コーポレーション) 2003. 03. 14, 【0027】 (ファミリーなし)	5-11